Z.I.V.
Zeitschrift zur Informationsverarbeitung

Speicher

Datenexplosion und Digitalisierung als Herausforderungen

Sehr geehrte Leserinnen und Leser!

Geht es Ihnen auch manchmal so, dass Sie mit Begriffen konfrontiert werden, die Ihnen in dem jeweiligen Bedeutungszusammenhang völlig absurd erscheinen? Oder erleben Sie es, dass bei Tagungen und in den Medien aneinander vorbeigeredet wird, mit offensichtlichen Worthülsen, die von allen Gesprächsteilnehmern mit anderen Inhalten gefüllt werden?

Ich hatte dieses Gefühl schon oft – aktuell habe ich mit der „Digitalisierung“ eine intensive Episode durchlebt. Da der Mensch aber lern- und anpassungsfähig ist, gewöhnt er sich daran, erschließt sich das neue Buzz Word und verbindet es mit Konzepten und Bedeutungen, die sich sukzessive einem dazu gerade entstehenden Konsens anpassen. Nachdem ich dieses Phänomen mit „ASP“, „Grid“ und „Cloud“ schon durchgemacht habe, konnte ich die Digitalisierung ganz gut wegstecken und habe sie bereits stilsicher in mein rhetorisches Repertoire integriert und den IT-Sektor meines Welterklärungsmodells an ihr ausgerichtet. Dies ist ja auch mehr oder weniger überlebenswichtig in der IT.

Kürzlich antwortete ein Redner während einer Veranstaltung zur Zukunft der Hochschul-IT auf die Frage, was den Unterschied zwischen einer Digitalisierungs- und einer IT-Strategie ausmacht, dass das – abgesehen von einem etwas stärkeren Fokus der Digitalisierung auf das Umfeld der jeweiligen Einrichtung und die digitale Interaktion – im Wesentlichen dasselbe wäre, das neue Buzz Word aber mehr finanzielle Möglichkeiten eröffne. Mir ist aber auch klar geworden, dass es nicht nur um Begrifflichkeiten und wirtschaftliche Aspekte geht: Wenn man sich das Narrativ der Digitalisierung erst einmal zu Eigen gemacht hat, erschließt es durchaus den Blick auf die zukünftig bestimmenden Handlungsfelder in der IT.

Mit der immer umfassenderen Nutzung von digitalen und vernetzten Geräten (Internet of Things), der grenzenlosen Kommunikation, der steigenden Verfügbarkeit von Daten und der zunehmend automatisierten Filterung und Aufbereitung dieser Daten, angepasst an unsere persönlichen Bedürfnisse und die aktuelle Situation, werden auch an Hochschulen komplett neue Szenarien in der Wissensvermittlung und der Forschung möglich – neue „Geschäftsmodelle“. Gleichzeitig birgt dieser Wandel natürlich auch neue Herausforderungen für die IT-Sicherheit und die nutzergerechte Ausgestaltung der IT-Services.

An der WWU beschäftigt sich aktuell eine Arbeitsgruppe des Rektorats damit, den Digitalisierungsaspekt für den Hochschulentwicklungsplan der WWU zu erarbeiten. Vertreter der IT-Einrichtungen und der IT-Nutzer haben sich zudem zu einer „Projektgruppe Digitalisierung“ zusammengefunden, in der sie sich regelmäßig zu aktuellen Entwicklungen austauschen und die Aktivitäten ihrer Einrichtungen abstimmen. Wenn man sich mit der Begrifflichkeit der „Digitalisierung“ einmal angefreundet hat, wird einem klar, dass sie einen Transformationsprozess unseres Arbeitsumfeldes, ja unserer ganzen Gesellschaft beschreibt, der uns mindestens für ein Jahrzehnt begleiten wird.

Herzlichst,
Ihr Raimund Vogl

Titelthema

Aktuelles

Ständige Rubriken

Titelthema

Speicher

Wenn man im Kontext der Informationstechnik von Speichern spricht, so geht es meist um Arbeits- oder Datenspeicher und damit letztlich um Leistungsfähigkeit und Speicherkapazität. Es geht aber auch um den Vorgang des Speicherns und alle Fragen, die dieser Prozess aufwirft – insbesondere vor dem Hintergrund einer wahren Datenexplosion in den vergangenen Jahren und veränderter Rahmenbedingungen für Datenverfügbarkeit, Datenschutz und Privatsphäre. Welche Daten besitze ich? Welchen Wert haben diese Daten für mich? Welchen für andere? Wo speichere ich sie? Festplatte, USB-Stick, externer Speicher, Cloud-Dienst? Wie sicher sind sie dort? Wie gut sind sie gegen Datenverluste geschützt? Wie viele Kopien benötige ich? Wie schnell und von wo kann ich auf sie zugreifen? Diese Fragen machen deutlich, wie viele Entscheidungen eine Einzelperson bewusst oder unbewusst beim Speichern von Daten trifft. Für Einrichtungen wie die WWU sind noch viele andere Aspekte relevant, da hier sehr große Datenmengen verarbeitet und verwaltet werden müssen und personen- und forschungsbezogene Daten besonders schützenswert sind.

Das Thema „Speicher“ ist sehr weitläufig, sodass die Z.I.V. nur einen Einblick in Bereiche geben kann, die an der WWU bedeutsam sind: Hierzu gehören insbesondere die Verfügbarkeitsstrukturen an der WWU, deren Zukunft das Ceph-Speichersystem sein könnte, sowie der Umgang mit Forschungsdaten, der sich derzeit im Wandel befindet und grundsätzliche Entscheidungen erfordert. Hier spielt auch der Clouddienst sciebo eine Rolle, dessen Weiterentwicklung das Team um Holger Angenent vorantreibt.

Datenverfügbarkeit an der WWU

Backup ist so letztes Jahrzehnt!

von Stefan Ost

Die Menge an gespeicherten Daten wächst unaufhaltsam, gleichzeitig steigen die Erwartungen im Hinblick auf die Verfügbarkeit: Nutzer wollen jederzeit, überall, von einem beliebigen Gerät zuverlässig und idealerweise auch noch unter Wahrung der Privatsphäre auf ihre Daten zugreifen. Um diesen veränderten Ansprüchen gerecht zu werden, hat die WWU ihr Konzept zur Datenverfügbarkeit in den letzten Jahren grundlegend verändert. Das hat Auswirkungen auf die Ausgestaltung der System-Architektur, das sogenannte Client-Server-Computing, das Rechner in zwei Gruppen unterteilt: Server, die Daten zur Verfügung stellen, und Clients (bspw. Ihr Arbeitsplatzrechner oder auch Ihr Smartphone), die auf die Daten zugreifen und sie verarbeiten.

In den 90er Jahren war Speicher vergleichsweise teuer, ein Datenbackup erfolgte daher nicht zuletzt aus betriebswirtschaftlichen Gründen auf externen Medien, in der Regel auf Magnetbändern. An der WWU wurde das Abschreiben (Backup) und Zurückspielen (Restore) von Daten durch eine zentrale Infrastruktur aus Band-Robotern und Servern unterstützt und durch die Software TSM (Tivoli Storage Manager) abgewickelt, die auch heute noch im Einsatz ist. In einem solchen System waren die Daten verfügbar, solange der Server verfügbar war. Verlor der Server – beispielsweise durch einen Defekt – gespeicherte Daten, so konnten diese nach der Fehlerbehebung von den Bändern zurückgespielt werden. Erst nach Abschluss dieser Maßnahmen standen der Server und damit die Daten wieder zur Verfügung. Eine Betriebsunterbrechung von mehreren Stunden wurde damals als unvermeidlich akzeptiert.

Heute ist die Situation anders: Aktuelle File-Server stellen riesige Datenmengen im Bereich von 10 TB und mehr zur Verfügung, das heißt ein Zurückspielen des Gesamtdatenbestands würde selbst bei einer sehr schnellen Netzwerkverbindung mehrere Tage dauern. Die damit verbundene Betriebsunterbrechung ist mittlerweile jedoch nicht mehr akzeptabel. Um das Verfügbarkeitsproblem zu lösen, werden Daten daher nicht länger nur auf Bändern gesichert, sondern mehrfach auf unterschiedlichen Servern gespeichert – man spricht von einer Spiegelung der

Daten. Ein Ersatz-Server kann mit wenigen Handgriffen in Betrieb genommen werden und die Betriebsunterbrechung bleibt kurz.

Allerdings ist das Verfahren mit einem enormen Mehrbedarf an Speicher verbunden, da sich der ohnehin große Platzbedarf vervielfacht. So werden die Daten des zentralen Groupware-Systems Exchange (E-Mails, Kontakte, Termine, usw.) beispielsweise vierfach gespeichert: je zwei Kopien in zwei geografisch getrennten Serverräumen. Zur Sicherheit, aus gutem Grund „last-line-of-defense“ genannt, werden die Daten zusätzlich auch noch auf Bänder abgeschrieben, die sich an einem dritten Standort befinden. Vor diesem Hintergrund verwundert es nicht, dass das TSM-Backup-Volumen an der WWU bereits seit 2010 kleiner ist als die Menge des installierten Speichers (Abb. 1).

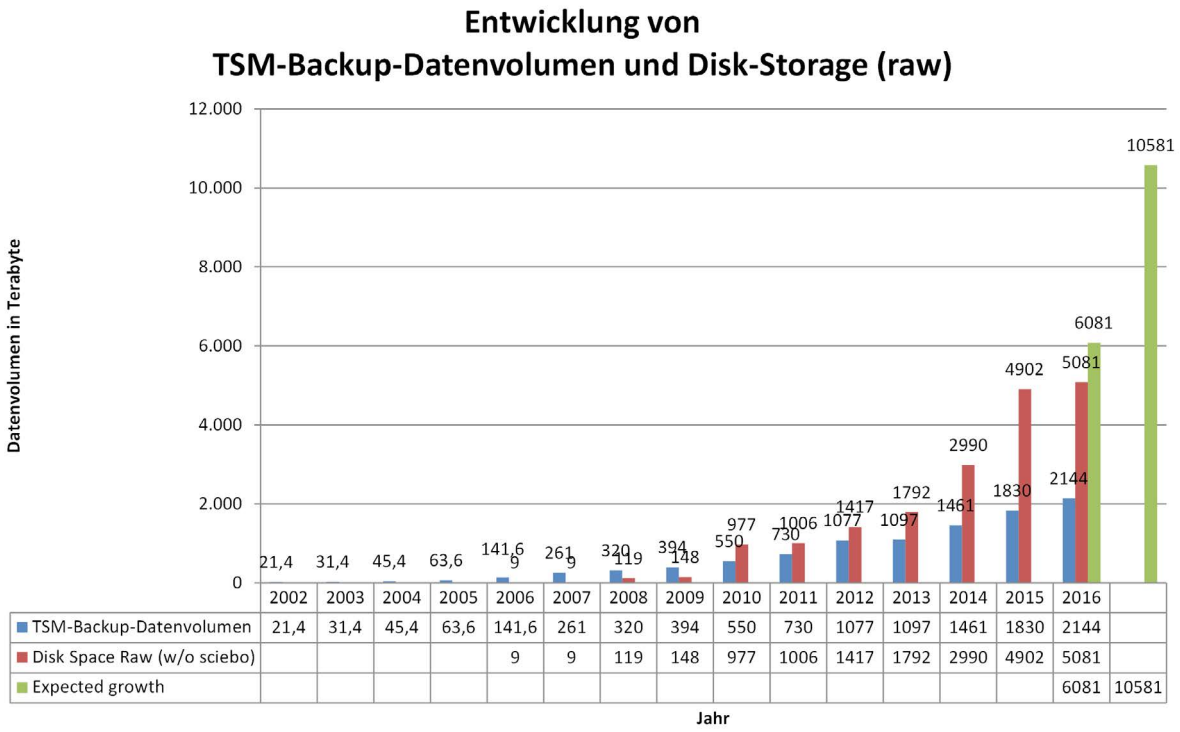


Abb. 1: Entwicklung des TSM-Backup-Datenvolumens von 2002 bis 2016

Beim Cloudspeicherdienst „sciebo“ wird eine etwas andere Strategie verfolgt: Die bei sciebo gespeicherten Daten werden zentral nur einmal gesichert; eine hohe Datenverfügbarkeit wird aber dennoch durch die Kombination von server- und clientseitiger Speicherung erreicht. Die Daten liegen dabei nicht nur auf den sciebo-Servern, sondern werden auch auf alle PCs und Laptops kopiert, auf denen der Nutzer seine Daten synchronisiert.

Wie langlebig die aktuellen Verfügbarkeitskonzepte sein werden, hängt im Wesentlichen von der weiteren Entwicklung der Datenmengen an der WWU ab – ein zunehmendes Wachstum erscheint allerdings wahrscheinlicher als eine Stagnation. Das ZIV muss sich der Herausforderung, Daten für die Nutzer verfügbar zu halten, also auch in Zukunft stellen und technische Fortschritte sowie neue Verfahren im Bereich der Datenspeicherung weiterhin im Blick behalten.

Ceph – Die Zukunft der Datenspeicherung?

von Stefan Ost

Wie der Artikel zur Datenverfügbarkeit zeigt, wächst der an der WWU installierte Speicher exponentiell. Damit steigen auch die Beschaffungs- und Betriebskosten im Speicher-Umfeld und es stellt sich die Frage, wie man Speicher kostengünstiger als bisher zur Verfügung stellen kann. Um eine Lösung zu finden, muss man zunächst die Kostenfaktoren von traditionellen Speicher-Servern identifizieren: Auf der einen Seite zählen hierzu die Server-Hardware (Prozessoren, Speicher, Festplatten, SSDs usw.) sowie deren Wartung (inkl. Austausch defekter Komponenten), auf der anderen Seite entstehen Kosten auch durch Software-Lizenzen und Software-Wartung.

Auf Grund von fehlender Konkurrenz gibt es bei der Hardware kaum Einsparpotential. Weltweit existieren nur wenige Hersteller von Speicherkomponenten, sodass alle Anbieter von Speicherservern ihre Komponenten letztlich von den gleichen Herstellern beziehen. Der Austausch defekter Komponenten ist im Wesentlichen ein Liefer-Service und kann von vielen Anbietern effizient angeboten werden. Auch bei der Wartung ist das Einsparpotential also gering. Die Funktionalität von Speicherservern wird aber nicht primär durch die Hardware, sondern durch die Software bestimmt, die auf ihnen läuft. Hier können sich Hersteller von der Konkurrenz abheben, indem sie reizvolle Funktionen anbieten. Diese lassen sie sich jedoch gut bezahlen. Kann man solche Kosten vermeiden, indem man – nach dem Vorbild des freien Linux-Server-Betriebssystems – lizenzkostenfreie Software nutzt? Ja, man kann: Ceph ist eine freie Software zum Betrieb von Speicher-Servern.

Ein ceph-Cluster besteht aus konventionellen Servern, die mit lokalen Speichermedien (Festplatten oder SSDs) ausgerüstet sind. Als Beispiel gehen wir von 10 Servern aus. Jeder Server habe 12 Festplatten mit einer Kapazität von 6 TB. Insgesamt also 72 TB pro Server und 720 TB pro Cluster. Gekoppelt sind die 10 Server untereinander mit einem schnellen (40 Gbs) Ethernet-Datennetz. Ceph verbindet diese Einzel-Komponenten zu einem Gesamtsystem, dem ceph-Cluster. Gemäß einem Regelsatz, der sogenannten „Pla-

cement Policy“, werden die Datenobjekte gespeichert. Ein einfacher Regelsatz wäre zum Beispiel:

1. Speichere jedes Datenobjekt mit drei Kopien.
2. Kein Datenobjekt darf doppelt auf einer Festplatte gespeichert werden.
3. Kein Datenobjekt darf doppelt auf dem gleichen Server gespeichert werden.

Fällt eine Festplatte aus, stellt Regel 2 sicher, dass es von diesem Datenobjekt noch zwei weitere Kopien auf anderen Festplatten gibt. Fällt ein ganzer Server aus, und damit seine 10 lokalen Festplatten, so gibt es von allen Datenobjekten, die auf allen Festplatten des ausgefallenen Servers gespeichert waren, auf den verbleibenden Servern noch mindestens 2 Kopien (Regel 3). Im Hintergrund überwacht ceph kontinuierlich die Einhaltung des Regelsatzes für alle Datenobjekte und sorgt bei Ausfall eines Speicherortes automatisch für Abhilfe durch das Anlegen neuer Kopien. Mit diesem Regelsatz ist man also gegen den gleichzeitigen Ausfall von 2 Festplatten oder von 2 Servern geschützt. Allerdings reduziert sich die Speicherkapazität des Clusters auf ein Drittel (240 TB) der ursprünglichen 720 TB Gesamtkapazität.

Es sind andere Regelsätze denkbar, die auf Kosten von erhöhtem ceph-internen Aufwand sparsamer mit der Speicherkapazität umgehen. Der ceph-Administrator wählt den Regelsatz passend zu den Anforderungen der Anwendung aus. Ceph ist allerdings nichts für den kleinen Speicherhunger: Kleinere Cluster haben eine Kapazität von 100 TB, große Installationen, wie etwa die am CERN, sind 50 PB groß und wachsen ständig. Das Vergrößern und Verkleinern eines ceph-Clusters ist sehr einfach möglich, indem man einen weiteren Server hinzufügt oder einen vorhandenen Server abschaltet. Beim Verkleinern sorgt ceph automatisch für das Erzeugen fehlender Kopien auf den verbliebenen Servern. Diese Eigenschaft ist auch in Bezug auf eine Server-Erneuerung nach einigen Betriebsjahren sehr attraktiv: Man fügt die neuen Server zum ceph-Cluster hinzu und schaltet anschließend nach und nach die alten Server ab. Am Ende dieses Prozesses hat man – ohne Betriebsunterbrechung – die Daten des ceph-Clusters auf neue Hardware migriert.

Mehr Durchblick beim Forschungsdatenmanagement

Neues Forschungsdatenportal der WWU hilft bei Fragen weiter

von Dominik Rudolph

Die Datenexplosion der letzten Jahre macht auch vor der Forschung nicht halt. Die Digitalisierung hat zu einem enormen quantitativen und qualitativen Wachstum von Forschungsdaten – wie zum Beispiel Textdaten, Messdaten, Daten aus Erhebungen oder aus medizinischen Proben – geführt. Gleichzeitig wächst das Bewusstsein für den langfristigen Wert dieser Daten: Sie werden nicht länger nur als flüchtiges „Abfallprodukt“ des Forschungsprozesses angesehen, sondern als wichtige Ressource für zukünftige Forschungsvorhaben, die kostenintensive, redundante Forschung vermeidet und der Qualitätssicherung und Kontrolle erzielter Ergebnisse dient. Dies spiegelt sich auch in den Forderungen und Richtlinien wichtiger Organisationen und Einrichtungen wie der Deutschen Forschungsgemeinschaft (DFG), der Hochschulrektorenkonferenz (HRK), der Allianz der deutschen Wissenschaftsorganisationen und des Rates für Informationsinfrastrukturen (RfII) wider. In der Regel fordern sie eine Langzeitarchivierung von mindestens zehn Jahren, die Erstellung von konkreten Datenmanagementplänen bei der Projektplanung und möglichst freien Zugang zu den Daten.

In der Praxis ergeben sich für die Forschenden an der WWU allerdings zahlreiche Fragen: Wie lassen sich die Daten für diesen Zeitraum sicher speichern und zwar so, dass sie auch in zehn Jahren noch lesbar sind? Gerade gerätespezifische Daten liegen oft in sehr speziellen Formaten vor, die sich mit neuen Geräten nicht mehr ohne weiteres öffnen lassen. Riesige Datengrößen und -mengen, wie sie beispielsweise bei mehrjährigen Simulationsexperimenten in der Geoinformatik entstehen, sind ein weiteres Problem. Welche rechtlichen Aspekte sind zu beachten? Dürfen die Daten überhaupt zugänglich gemacht werden und unter welchen Bedingungen? Hier muss das Thema Datenschutz berücksichtigt werden, dessen Relevanz bei Erhebungen mit Probanden in der Psychologie oder mit Patienten in der Medizin besonders deutlich wird. Bei Kooperationsprojekten mit anderen Hochschulen oder Firmen stellt sich auch die Frage nach dem Eigentum der Daten. Wie muss ein Datenmanagementplan aussehen? Welche Vorteile bringt ein gutes Forschungsdatenmanagement? Und lohnen sich Zeit- und Arbeitsaufwand?

Antworten auf diese und weitere Fragen gibt das neue Forschungsdatenportal der WWU, das gemeinsam von der ULB, dem ZIV und dem Forschungsdezernat betrieben wird. Dort gibt es neben Kontaktmöglichkeiten auch zahlreiche Infos rund um das Speichern, Zitieren und Auffinden von Forschungsdaten sowie konkrete Handreichungen und Musterbeispiele. Geplant ist außerdem eine Forschungsdatenrichtlinie der WWU, die den Umgang mit Forschungsdaten regelt. Orientiert an den Richtlinien guter wissenschaftlicher Praxis sind die Forschenden dazu aufgerufen, Verantwortlichkeiten und rechtliche Aspekte zu klären und in einem Datenmanagementplan festzulegen, entstandene Daten zu dokumentieren und die Daten – sofern möglich – öffentlich zu machen. Die hierzu notwendigen technischen Infrastrukturen und Beratungsangebote schafft die WWU.

Von Supercomputern und Cloudspeichern

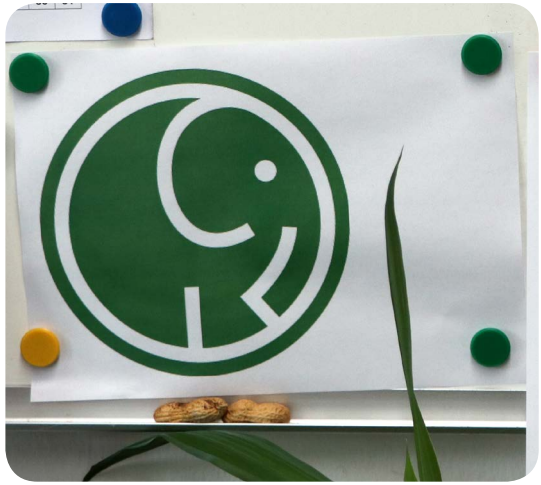
Zu Besuch bei Holger Angenent vom Bereich Systembetrieb

von Anne Thoring

Am Whiteboard hängt ein grüner Elefant, ausgedruckt auf Papier, in der Stiftablage darunter liegen zwei Erdnüsse. Was wie Zufall aussieht, ist eine augenzwinkernde Hommage an sciebo, die Campuscloud, die zahlreiche Hochschulen in NRW ihren Studierenden und Mitarbeitern gemeinsam anbieten. Im Büro von Holger Angenent hat das Projekt in gewisser Weise seinen Hauptwohnsitz, denn als technischer Verantwortlicher betreut der Physiker den Cloud-Dienst bereits seit der Ideenfindung. Seit 2010 arbeitet Angenent am ZIV im Bereich „Systemdienste“, der die notwendige Infrastruktur für sciebo und einen Großteil der anderen ZIV-Services bereitstellt. Das Aufgabenspektrum der 16 Mann starken Abteilung reicht von der Beschaffung der Hardware über die Installation systemnaher Anwendungen, das Identitätsmanagement und den Betrieb von Datenbanken, Webservern und HPC-Systemen bis hin zur Optimierung von Rechnern und Betriebssystemen.

Ursprünglich wurde Angenent als HPC-Analytiker angestellt – und HPC ist, neben sciebo, immer noch ein zentrales Standbein seiner Arbeit. Das Kürzel steht für High Performance Computing, also Hochleistungsrechnen. Mit PALMA und PHICUS gibt es am ZIV derzeit zwei Hochleistungsrechner, die – dank einer großen Anzahl von Prozessorkernen und sehr viel Hauptspeicher – überaus komplexe wissenschaftliche Problemstellungen lösen können. Besonders häufig werden sie von Forschern aus den Fachbereichen Physik, Chemie, Biologie, Informatik und in den Wirtschaftswissenschaften verwendet. „Supercomputer überschreiten die Leistungsgrenze normaler Desktop-PCs deutlich, aber vom Grundprinzip sind beide erstaunlich ähnlich“, erläutert Angenent. Dies spiegelt sich auch bei der Betreuung des HPC-Systems wieder, denn genau wie beim Arbeitsplatzrechner müssen Betriebssysteme und Benutzersoftware aufgespielt und regelmäßig aktualisiert werden.

Unterschiede ergeben sich vor allem durch den Einsatz der Hochleistungsrechner im Forschungskontext. So werden beispielsweise je nach Fachbereich und konkretem Projekt sehr spezifische Simulations- und Auswertungsprogramme benötigt, teilweise müssen die Projektteams ihre Software sogar selbst entwickeln. Als HPC-Experte hält Holger Angenent daher regelmäßig Vorlesungen zur Programmierung wissenschaftlicher Software und berät Nutzer bei der Anwendung des



Bei Holger Angenent wird nicht nur das sciebo-Maskottchen mit Erdnüssen versorgt, auch der Dienst selbst ist hier in guten Händen.

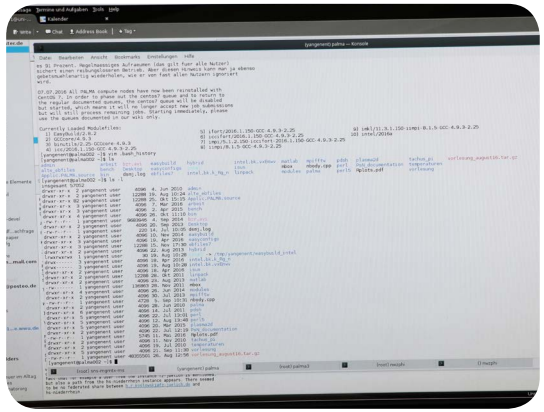
HPC-Systems. Rechenprozesse dauern nicht selten mehrere Stunden oder Tage, sodass ganze Forschungsprojekte mit der Verlässlichkeit und Funktionstüchtigkeit der Supercomputer stehen und fallen. Am PC hat Angenent daher immer auch ein Auge auf Ganglia, ein System zur Serverüberwachung. Entspricht der Ist-Zustand den Erwartungen, ist das aber kein Grund zum Ausruhen, denn Angenent ist nicht nur Praktiker, sondern auch Wissenschaftler: Ihn beschäftigt die Frage, wie sich ein modernes HPC-System aufsetzen lässt und welche Weiterentwicklungen dazu nötig sind.

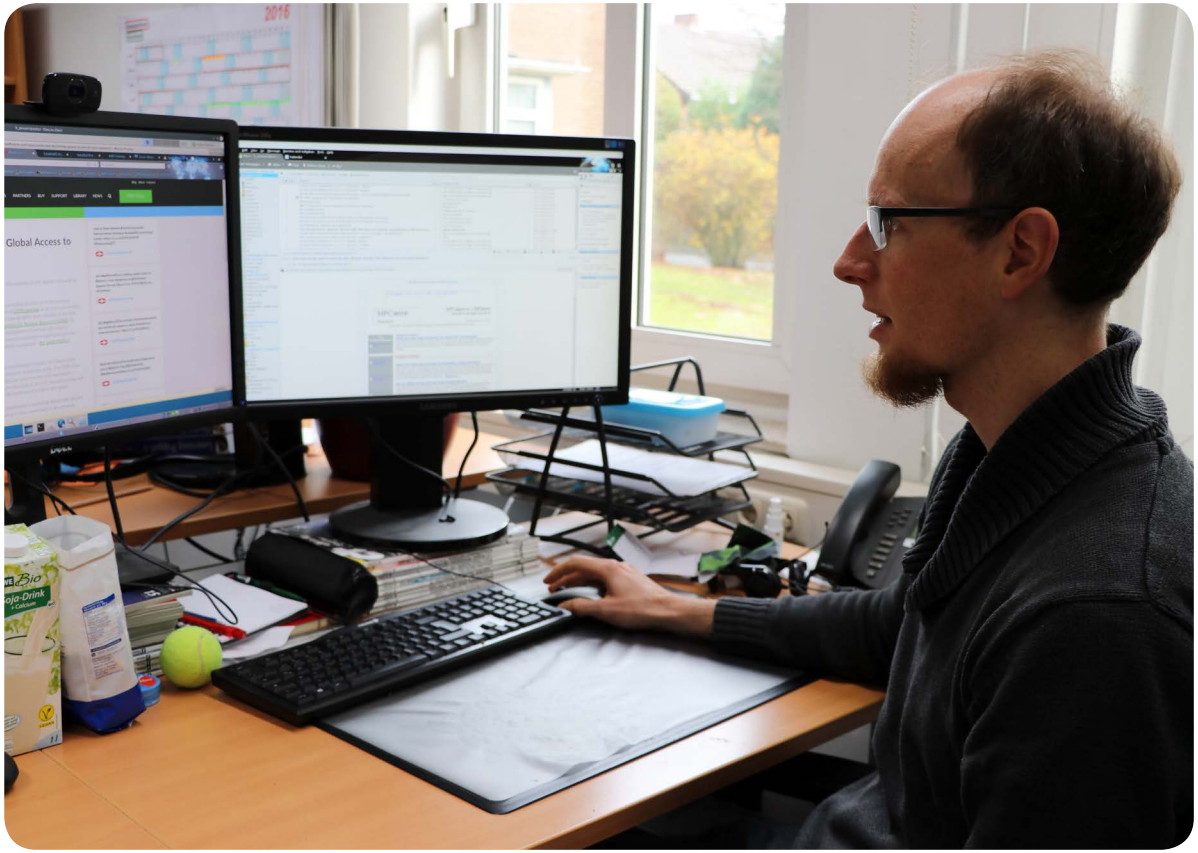
Zukunftsorientiert arbeitet der Physiker aber nicht nur im Bereich High Performance Computing – mit dem Forschungsprojekt „sciebo“ durfte Angenent im Bereich Cloud Computing Neuland betreten. Von Beginn an hatte die Campuscloud andere Dimensionen als das hochschulinterne Sync & Share-Projekt der TU Berlin und war nur mit bwSync&Share, der Hochschul-Cloud von Baden-Württemberg, wirklich vergleichbar. „Mit nur einer konkreten Vergleichsmöglichkeit war es sehr schwierig zu entscheiden, welche Soft- und Hardware-Komponenten sich am besten eignen und zukunftssicher sind“, berichtet Angenent von den Anfängen des Projekts. Der Erfahrungsaustausch

In den Serverräumen der WWU ist Angenent nur selten, Wartung und Fehlerbehung erfolgen normalerweise über den Dienstrechner vom Schreibtisch aus.

mit den Cloud-Betreibern in anderen Bundesländern war zu Beginn sehr wichtig, doch ab einem gewissen Punkt zählten vor allem intensive Recherche sowie eigene Experimente mit Testsystemen.

Viel Zeit haben Angenent und seine Kollegen daher in den Produktvergleich investiert, bevor die Entscheidung für das Open Source Produkt ownCloud gefallen ist. „Teil einer Open Source Community zu sein, war ein wichtiges Argument“, erläutert Angenent die Hintergründe. „sciebo ist ja nicht nur ein Dienst, den wir anbieten, sondern auch ein Forschungsprojekt, bei dem der Aufbau und die Weiterent-





Für seine Arbeit nutzt Angenent gleich drei Bildschirme: Auf dem ersten schreibt der Physiker Skripte und recherchiert für anstehende Projekte, auf dem zweiten beantwortet er eingehende Nutzeranfragen und auf dem dritten überwacht er den Betrieb von Cloud- und HPC-Systemen.

wicklung dieses Dienstes im Zentrum stehen.“ Zum Aufbau gehört neben der Software auch eine passende Hardware. Vor der Beschaffung wurden die Systeme verschiedener Hersteller intensiv getestet und verglichen. Um eine optimale Performance und Verlässlichkeit zu erzielen, muss die Hardware-Architektur so genau wie möglich auf die Software und den speziellen Anwendungsfall zugeschnitten sein. Doch nicht nur die Auswahl der Produkte, auch die Konfiguration spielt eine entscheidende Rolle und ist mit viel Arbeit verbunden. Für den Betrieb von sciebo musste das kleine Team um Holger Angenent unter anderem die Webserver einrichten, Datenbank-Cluster aufsetzen, Speicherplatz im Petabyte-Bereich bereit-

stellen und Load Balancer für die Ausfallsicherheit vorschalten.

Nach fast drei Jahren Vorbereitungszeit wurde die Campuscloud Anfang 2015 schließlich an 16 Hochschulen offiziell gestartet – für Angenent eine stressige Zeit, da viele Probleme kurzfristig gelöst werden mussten. In solchen Phasen, aber auch wenn es um die Entwicklung von Problemlösungsstrukturen im Allgemeinen geht, profitiert Angenent von seinem Physik-Studium: „Was man in der Physik letztlich lernt, sind Problemlösungsskills. Um handlungsfähig zu bleiben, reduziert man komplexe Dinge auf Einfaches." Um Überschaubarkeit geht es auch bei der Weiterentwicklung von sciebo, denn die Liste an Möglichkeiten ist lang. Um bei der Optimierung effizient zu sein und Fortschritte zeitnah zur Produktionsreife zu bringen, ist eine schnelle Auffassungsgabe entscheidend. Als Organisator aller technischen Angelegenheiten behält Angenent aber auch die Nutzerwünsche und das Leistungspotential des kleinen sciebo-Teams im Blick und setzt auf dieser Basis Prioritäten: „Unsere To-Do-Liste umfasst derzeit Experimente zur strukturellen Weiterentwicklung von sciebo und eine Verbesserung der Sicherheitsmechanismen, des Monitoring-Systems und der Datenauswertung."

Sciebo und HPC, HPC und sciebo – die Hauptsäulen seiner Arbeit sind für Angenent wie zwei Seiten derselben Medaille: „Die technischen Systeme sind sich sehr ähnlich, daher ist es absolut sinnvoll, dass ich in beide Bereiche involviert bin. Gleichzeitig sind die Nutzungsszenarien und Anforderungen aber sehr unterschiedlich, fast schon gegensätzlich." Das HPC-System ist auf wenige, arbeitsintensive Anfragen ausgelegt und wird von etwa 100 Wissenschaftlern verwendet, die meist technisches Vorwissen mitbringen. Sciebo dagegen nutzen zehntausende Studierende und Mitarbeiter mit unterschiedlichsten Vorkenntnissen für ihre alltägliche Arbeit, sodass das Cloud-System mit vielen kurzen Anfragen zurechtkommen muss. Bei der Betreuung muss Angenent daher mit zweierlei Maß messen: „Wenn das HPC-System zu annähernd 100 Prozent ausgelastet ist, ist das optimal – bei sciebo wäre das der Katastrophenfall." Gerade dieses Spannungsfeld eröffnet aber auch neue Perspektiven und ist ein Impulsgeber für die wissenschaftliche Arbeit.

Auf Tagungen und Konferenzen trifft man Holger Angenent in den letzten Jahren zunehmend häufiger, denn der Austausch mit anderen Hochschulen, Forschungseinrichtungen und Softwareherstellern ist zu einem wichtigen Teil seiner Tätigkeit geworden. Nur wer von seinen Erfahrungen berichtet und auf dem Laufenden bleibt, kann auch Einfluss auf die Weiterentwicklung eines Produktes wie sciebo nehmen. Den Großteil der Zeit verbringt Angenent aber nach wie vor am Arbeitsplatzrechner, wo ihm eine fast schon spartanisch erscheinende Ausstattung genügt: „Für 90 Prozent der Aufgaben brauche ich lediglich einen Browser, ein E-Mail-Programm und eine Kommandozeile zum Schreiben von Skripten. Außer diesen drei Tools sind eigentlich nur noch Linux-Kenntnisse unentbehrlich." Mit wenigen Tools, viel Wissen und einer festen Überzeugung von den eigenen Projekten lässt sich eben auch vom Schreibtischstuhl aus einiges bewegen.

Erfahrungsaustausch und Zukunftsperspektiven

sciebo-Tag 2016 bringt Vertreter der Teilnehmereinrichtungen zusammen

von Holger Angenent

Zahlreiche Vorträge zur weiteren Entwicklung von sciebo und der Austausch zwischen den teilnehmenden Einrichtungen standen auf der Agenda des sciebo-Tags 2016, zu dem im vergangenen Herbst rund 50 Hochschulvertreter erschienen. Das vergangene Jahr verlief für die Campuscloud insgesamt erfolgreich: Mehr als 60.000 Personen an 27 Hochschulen in NRW haben sich mittlerweile für den Dienst angemeldet und die Nutzerzahl steigt konstant. Insbesondere zu Semesterstart registrieren sich viele Studierende, was auf eine gute Akzeptanz unter den Erstsemestern schließen lässt.

Um die Reichweite und die Zufriedenheit mit sciebo quantitativ zu untersuchen, wurde Ende 2015 eine Umfrage unter allen Nutzern durchgeführt – mit einer hervorragenden Resonanz von mehr als 16.000 Teilnehmern. Auch die Ergebnisse der Umfrage sind nach nur einem Jahr Laufzeit durchweg zufriedenstellend: Im direkten Vergleich mit kommerziellen Cloud-Diensten wie Dropbox, iCloud oder Google Drive schneidet sciebo am besten ab und kann insbesondere beim

Speichervolumen und beim Datenschutz punkten. Auch das Vertrauen in die Universitäten, die den Dienst anbieten, ist groß.

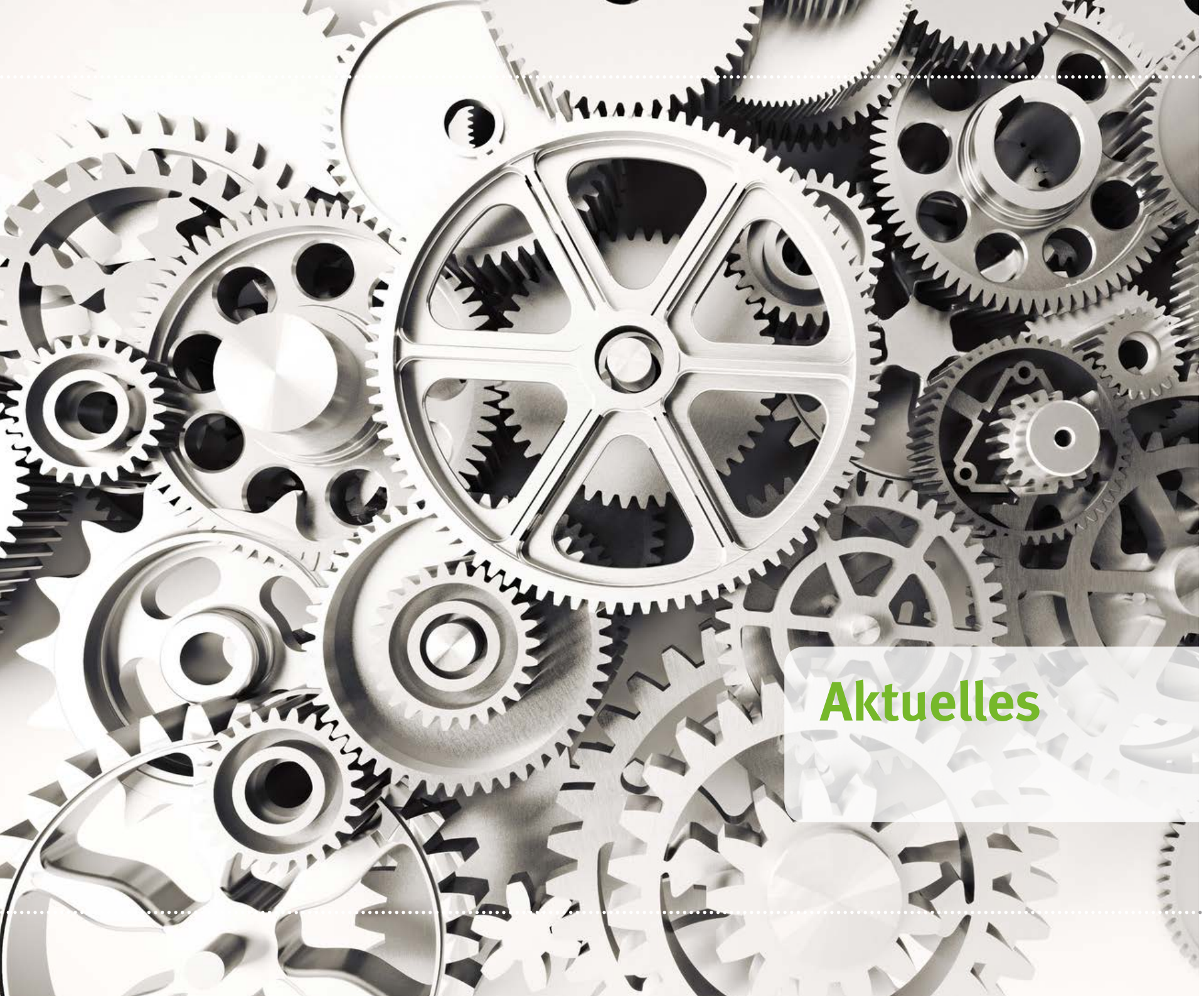
Als zentrale Argumente für die Etablierung eines eigenen Dienstes sind Sicherheit und ein hoher Datenschutz auch für die teilnehmenden Einrichtungen von entscheidender Bedeutung. Um den diesbezüglich sehr hohen Ansprüchen gerecht zu werden, muss sciebo stetig überprüft und weiterentwickelt werden. Anfang 2016 haben die Betreiber daher an allen Standorten eine Sicherheitsüberprüfung der Soft- und Hardwarekomponenten durchgeführt. Das Ergebnis dieses Audits fällt grundsätzlich positiv aus, kleinere Mängel (z.B. ein regelmäßiger Turnus bei der Installation von Betriebssystemupdates) konnten zeitnah behoben werden. Die Basis-Software ownCloud wird 2017 durch die Unterstützung der 2-Faktor-Authentifizierung zudem um ein wichtiges Sicherheitsfeature erweitert.

Um den Datenschutz darüber hinaus noch weiter auszubauen, wird eine Kooperation mit der Firma Skymatic angedacht, deren Open Source-Produkt Cryptomator eine Ende-zu-Ende-Verschlüsselung von ausgewählten Daten ermöglicht. Die Software richtet sich unter anderem an Nutzer, die bei der Speicherung von vertraulichen Daten besonders hohe Sicherheitsanforderungen haben. Da Cryptomator bereits frei verfügbar ist, können sciebo-Nutzer die Verschlüsselungssoftware auch unabhängig von einer Kooperation einsetzen. Die Desktopversion für Windows, MacOS oder Linux ist kostenlos, die Mobilversion für iOS oder Android dagegen kostenpflichtig.

Die Einführung eines Tools zum kollaborativen Arbeiten wird von vielen sciebo-Nutzern gewünscht, Überlegungen dazu stehen aber noch am Anfang. Möglich erscheint derzeit eine Integration der Software Collabora. Mit der angekündigten Version 2.0 können Office-Dokumente von mehreren Nutzern gleichzeitig im Browser bearbeitet werden. Da ein solches Feature einen großen Mehrwert für die sciebo-Nutzer hat und neue sinnvolle Nutzungsszenarien eröffnet, wird eine Finanzierung geprüft.

Ein Thema außer der Reihe, aber keinesfalls unwichtig für die weitere Entwicklung von sciebo, ist die interne Umstrukturierung der Firma ownCloud. Nachdem einer der Mitgründer die Firma Mitte 2016 verlassen und das Konkurrenzunternehmen nextCloud gegründet hatte, wurde die wirtschaftliche Tragfähigkeit von ownCloud in einigen Medienberichten angezweifelt. Im Rahmen von Gesprächen konnte ownCloud aber überzeugend darlegen, dass die Firma wirtschaftlich solide und zukunftssicher aufgestellt ist. Für sciebo hat die veränderte Unternehmenssituation somit keine direkten Konsequenzen.

Da alle Beteiligten den Austausch im Rahmen der Veranstaltung sehr wertschätzen, wird der sciebo-Tag voraussichtlich auch 2017 wieder stattfinden.



Aktuelles

2016 – Ein Rückblick in Zahlen

von Dominik Rudolph

Die Datenexplosion, die Ihnen bei der Lektüre dieser Z.I.V.-Ausgabe des Öfteren begegnet, lässt auch anhand der statistischen Daten des ZIV erkennen. Nachdem der Datentransfer vom und ins Internet bereits im Vorjahr um 40 Prozent gestiegen war, hat er 2016 nochmals um 34 Prozent zugenommen und erreicht nun kaum vorstellbare 3.590 TB. Auch das Datenvolumen in unserem Backupsystem wächst immer stärker: Waren es 2010 noch 550 TB, so ist die Zahl bis Ende 2016 um 420 Prozent auf 2.350 TB angewachsen. Alleine im letzten Jahr beträgt der Zuwachs etwa 28 Prozent. Die Datenmenge im Webauftritt der WWU umfasst mittlerweile 7.510 GB und ist damit 2016 ebenfalls erheblich gewachsen (+32%). Der Trend des Vorjahres (+40%) setzt sich also auch in diesem Bereich fort.

Der Datenanstieg ist am ZIV jedoch nicht nur quantitativ, sondern auch qualitativ erkennbar, da die voranschreitende Digitalisierung zunehmend höhere Anforderungen an die Infrastruktur stellt. Um dieser Entwicklung Rechnung zu tragen, wurden beispielsweise die WLAN-Accesspoints deutlich ausgebaut (+12%) und gegen leistungsstärkere Technik (HD-WLAN) ausgetauscht, die einer größeren Zahl an Endgeräten den drahtlose Zugriff auf das Internet ermöglicht. Der Ausbau des Netzes ging mit etwas niedrigeren, aber konstanten Wachstumsraten voran, auf nunmehr über 77.000 Anschlüsse (+9%). Schwerpunkt der Arbeiten im letzten Jahr war vor allem die Optimierung des Netzes im Hinblick auf die Ausfallsicherheit und Performance. Im Bereich Telekommunikation stieg das Auftragsvolumen 2016 um 18 Prozent – primär bedingt durch den aktuell anstehenden Austausch der Telefonanlage und den Umstieg auf Voice over IP. Der Bereich AVM konnte dank Sondermitteln zudem in den Hörsälen aktiv werden und die Medientechnik (Beamer, Akustik, Mediensteuerungen) auf den neuesten Stand zu bringen.

Mehr Daten bedingen auch eine höhere Rechenleistung, um diese Daten effizient verarbeiten zu können. Das wird nirgends besser sichtbar als beim High Performance Computing (HPC). Im vergangenen Jahr hat das ZIV PALMA 1.5 als Übergangssystems beschafft, das das in die Jahre gekommene PALMA-System so lange verstärkt, bis PALMA 2 im Laufe dieses Jahres einsatzbereit ist. Durch diese Maßnahme konnte die Gesamtleistung des HPC-Systems der WWU um 55 Prozent auf insgesamt 121 TeraFLOP/s gesteigert werden.

Die zunehmende Digitalisierung lässt sich auch an der Abnahme der Druckaufträge beobachten, die seit fünf Jahren um circa 20 bis 30 Prozent sinkt. Allerdings hat sich der Negativtrend 2016 mit „nur“ 11 Prozent Rückgang verlangsamt, das Seitenvolumen ist sogar nahezu konstant geblieben.

Zukunftssichere Technik, optimierte Struktur

Kolloquium beleuchtet die grundlegende Erneuerung des WWU-Kommunikationssystems

von Markus Speer

Gleich zwei Großprojekte standen im vergangenen November im Mittelpunkt des ZIV-Kolloquiums „Erneuerung des Kommunikationssystems der WWU“: die Neustrukturierung des Backbone-Netzes (LAN und WLAN) und dessen organisatorische und technische Konvergenz mit dem Telekommunikationsnetz durch eine Umstellung auf Voice over IP (VoIP). Etwa 80 mehrheitlich externe Teilnehmer besuchten die zahlreichen Vorträge, die zum einen die bedarfsbegründenden Grunddaten, den DFG-Antrag und die Finanzierung des Projektes erläuterten. Zum anderen wurden die Schwerpunkte des Netzentwicklungsplans, der Stand der Umsetzung und die Entwicklung der Kennzahlen sowie bevorstehende Maßnahmen und Themen für den Zeitraum ab 2019 vorgestellt. In vertiefenden Vorträgen erläuterten Mitarbeiter der Abteilung Kommunikationssystem und Vertreter der beteiligten Firmen außerdem konkrete Maßnahmen aus einzelnen Teilbereichen.

Mit der Ausarbeitung eines Netzkonzepts zur grundlegenden und umfassenden Modernisierung des Kommunikationssystems hat das ZIV bereits 2009 begonnen, seit Anfang 2011 wurde intensiv an der Umsetzung gearbeitet. Mit der Realisierung des Backbone-Netzes 2016 wurde ein wichtiger Meilenstein erreicht, sodass der Abschluss des Gesamtprojektes voraussichtlich planmäßig im Jahr 2018 erfolgen kann. Zentrale Errungenschaft des neuen Backbones ist die Regionalisierung des Netzes (Abb. 1), die die Ausbreitung von Störungen auf definierte geografische Bereiche beschränkt. Neben diesen Regionen wurden zudem eine DataCenter-Region und eine Service-Region eingerichtet, die jeweils auf verschiedene Standorte verteilt sind. Als Gerätetyp wird im neuen Backbone der HP12504 eingesetzt. Es wurde ein Konzept umgesetzt, das es ermöglicht das Gesamtnetz in Endgerätegruppen, sogenannte VPNs (Virtuelle Private Netze), zu unterteilen. Diese VPNs sind aus Sicherheitsgründen stark voneinander abgetrennt und nur über ein Next Generation Firewall System (NGFW) miteinander gekoppelt.

Das neue TK-Konzept der WWU sieht nicht nur eine technische, sondern auch eine organisatorische Zusammenführung von Daten- und Telekommunikation zu einem gemeinsamen Kommunikationssystem vor. Die Grundlage hierfür bietet das rein VoIP-basierte OpenScape Voice-System der Firma Unify, das die seit 20 Jahren betriebene Sopho iS 3000-TK-Anlage ablösen wird. Das neue, redundant aufgebaute VoIP-System stützt sich auf das Regionalisierungskonzept, das für das Backbone entwickelt wurde. Als zentraler Bestandteil kommt ein dediziertes, auf zwei Standorte geo-redundant verteiltes ESX-Cluster mit 20 virtuellen Servern für die verschiedenen TK-Funktionalitäten zum Einsatz. Bedingt durch die Lösungsarchitektur ändert sich zukünftig auch das Aufgabengebiet des TK-Administrators, der sich – über die klassischen Aufgaben hinaus – intensiv mit Server- und Softwarethemen befassen muss.

Parallel zur Realisierung der zwei Großprojekte Backbone-Erneuerung und VoIP-Umstellung schreitet der Ausbau der WLAN-Infrastruktur voran. Im Fokus steht dabei das Thema High Density (HD)-WLAN für Hochschullehre und Veranstaltungen.

Dank eines speziellen Designansatzes, der auf Komplexität verzichtet, konnte der Rollout des HD-WLAN äußerst effizient gestaltet werden: In einem ersten Schritt wurden 210 WLAN Access Points innerhalb kurzer Zeit montiert und versorgen nun knapp 8.500 Hörsaalplätze in 35 Hörsälen sowie Foyers in 16 Gebäuden mit einem HD-WLAN. Planungen zum WLAN im öffentlichen Raum lassen zudem eine noch flächendeckendere WLAN-Versorgung in diesem Jahr erwarten.

Ergänzend zu den praxisbezogenen Vorträgen präsentierte das Institut für Informatik Forschungserkenntnisse zum Thema „Software-Defined Networking an der Universität Münster“. Vorgestellt wurden ein SDN-Ansatz, der applikationsspezifische Anforderungen automatisch in netzwerkspezifische Metriken umsetzt, sowie Möglichkeiten mit SDN ein vom Sender kontrolliertes Multicast-Konzept zu realisieren. Ein Pilotprojekt, das zusammen mit dem ZIV durchgeführt wurde, befasst sich zudem mit einem SDN-basierten Netzzugangsschutz als Alternative zu IEEE 802.1X.

Die Folien der einzelnen Vorträge finden Sie hier.

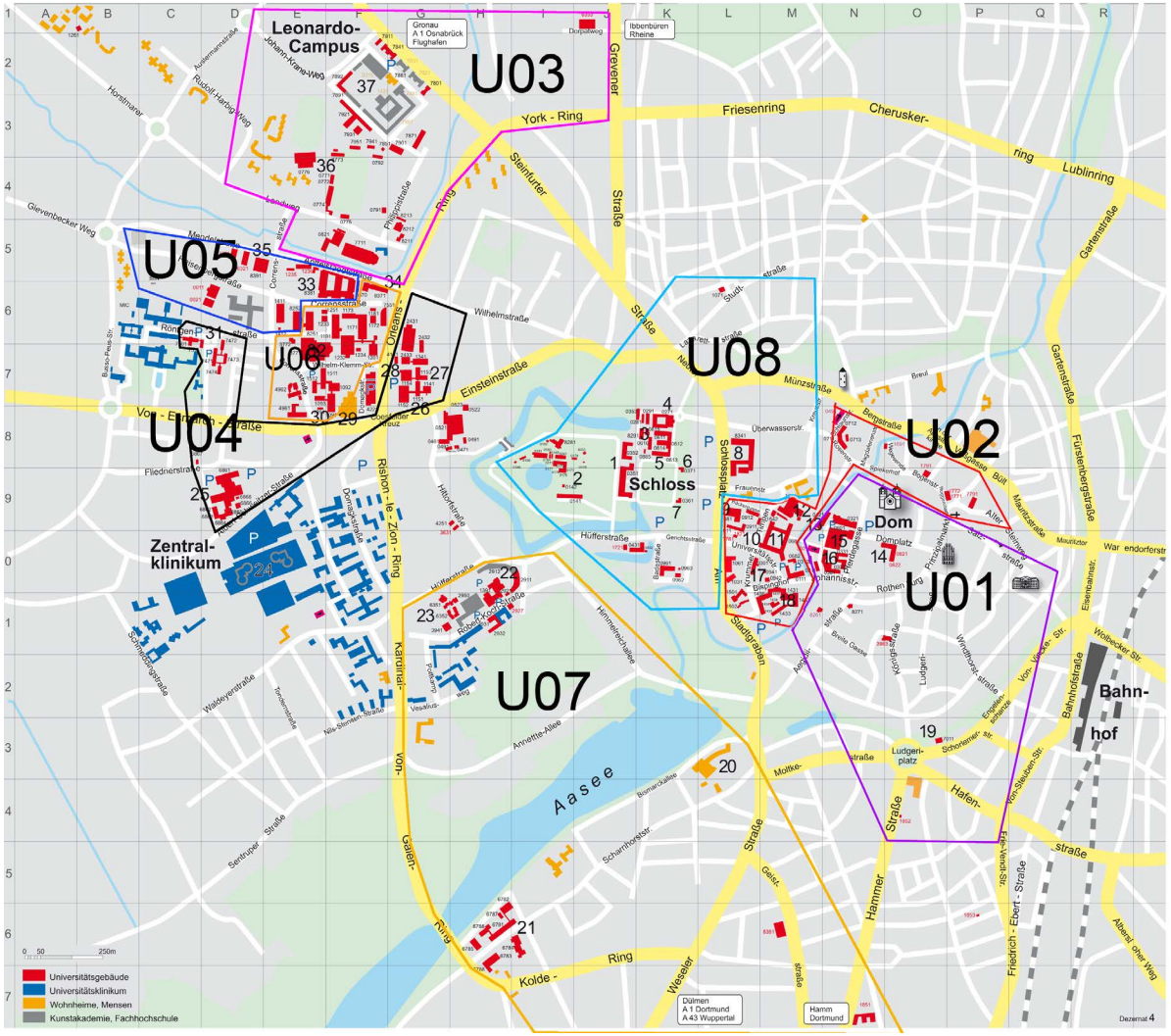


Abb. 1: Übersicht der einzelnen Regionen des Backbone-Netzes im Stadtplan

Whitelist statt Blacklist

Neues Verfahren beim Netzzugang erhöht die IV-Sicherheit

von Anne Thoring

Mehr Sicherheit im Netz der WWU verspricht das neue Whitelisting-Verfahren, mit dem das ZIV auf die veränderte Bedrohungslage und die zunehmenden Sicherheitsrisiken im Internet reagiert. Das Firewall-System der WWU folgt damit nicht länger einem liberalen Ansatz, bei dem die Rechner der WWU fast ohne Einschränkung weltweit erreichbar sind, sondern einer restriktiven Policy, die den Zugriff auf vernetzte Endgeräte von außen auf notwendige Ausnahmen beschränkt. Diese Ausnahmen bilden die sogenannte „Whitelist“. Die Nutzung von externen Diensten oder Systemen durch Rechner der WWU wird durch diese Maßnahme nicht eingeschränkt. Auch die gegenseitige Erreichbarkeit von Systemen der WWU und des Universitätsklinikums bleibt hiervon unberührt.

Um eine Beispielwirkung für andere IT-Bereiche der Universität zu erzielen, hat das ZIV seine Systeme Anfang Juli 2016 innerhalb von zwei Wochen vollständig auf das Whitelisting-Verfahren umgestellt. Dadurch konnte das Gefahrenpotential für die Systeme des ZIV in kürzester Zeit minimiert werden. Derzeit wird die Maßnahme auch auf alle anderen Bereiche der WWU ausgedehnt. Jede IVV definiert dazu eine eigene Whitelist mit Ausnahmen für die in ihrem IT-Bereich benötigten Dienste.

Noch Plätze frei im Lesesaal?

Der neue Platzticker der ULB

von Burkard Rosenberger

Die Arbeitsplätze in den Bibliotheken der WWU sind begehrt, und das nicht nur in den Lernphasen vor den Klausuren. Viele Studierende fragen sich deshalb oft, ob sich der Weg zur Bibliothek lohnt oder ob sie auf andere Arbeitsplätze ausweichen müssen. Doch welche Lern- und Arbeitsräume an der Universität bieten in einem solchen Fall noch freie Platzkapazitäten an?

Eine Antwort auf diese Frage liefert seit Juli 2016 der Platzticker, der im Rahmen eines Kooperationsprojekts von ULB und ZIV entstanden ist. Schnell und übersichtlich zeigt er freie Arbeitsplätze an derzeit fünf Bibliotheksstandorten: der Zentralbibliothek der ULB, der Bibliothek im Vom-Stein-Haus, den beiden Bibliotheken im Rechtswissenschaftlichen Seminar sowie der Fachbereichsbibliothek Wirtschaftswissenschaften. Da die Resonanz auf das neue Serviceangebot der ULB bislang durchweg positiv ist, ist eine Ausweitung auf weitere Standorte – insbesondere im Innenstadtbereich – bereits in Planung.

Die Idee, die dem Platzticker zugrunde liegt, ist relativ einfach: In einer großen Gruppe von Studierenden trägt statistisch gesehen ein nahezu konstanter Anteil mindestens ein Mobilgerät (z. B. Smartphone, Tablet, Notebook) bei sich, das sich ins WLAN der Universität einloggt. Dementsprechend ist die Anzahl der Personen in einem Raum proportional zur Gesamtzahl der WLAN-Logins in diesem Raum. Kennt man den Proportionalitätsfaktor, so lässt sich aus der Gesamtzahl der WLAN-Logins unmittelbar auf die Zahl der aktuell anwesenden Personen und – in einem weiteren Schritt – auf die Auslastung eines Raumes schließen (Abb. 1).

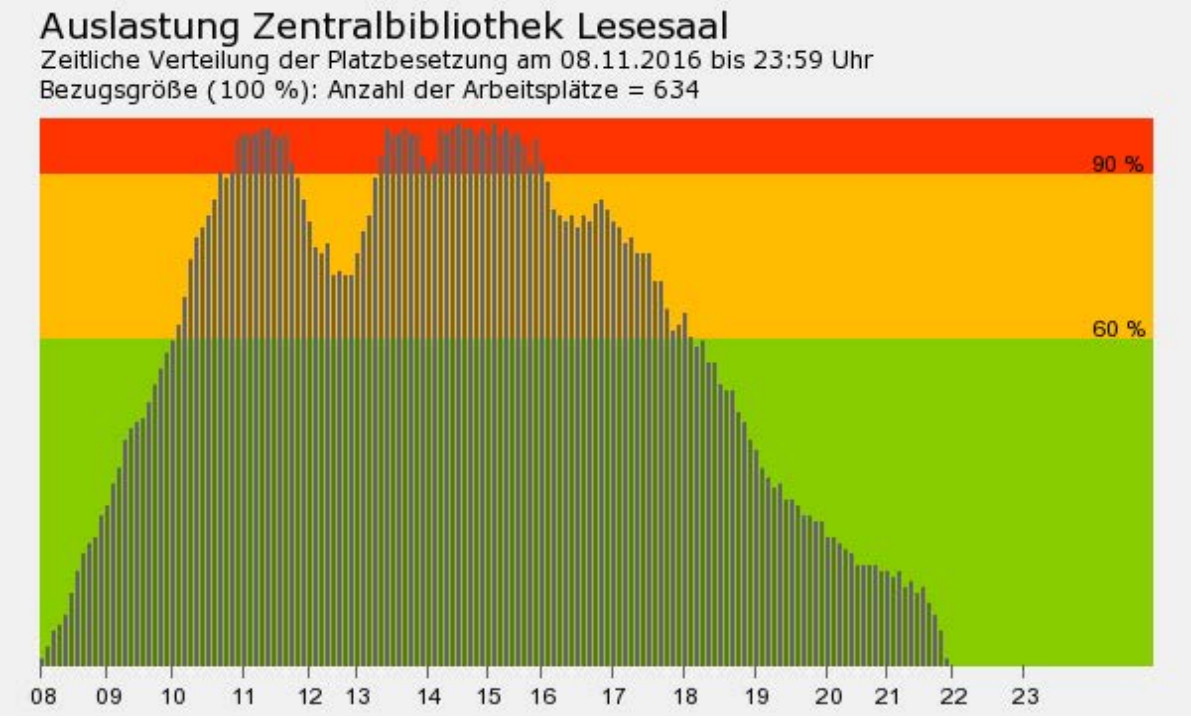


Abb. 1: Typische ermittelte Auslastungsquote für den Lesesaal der Zentralbibliothek

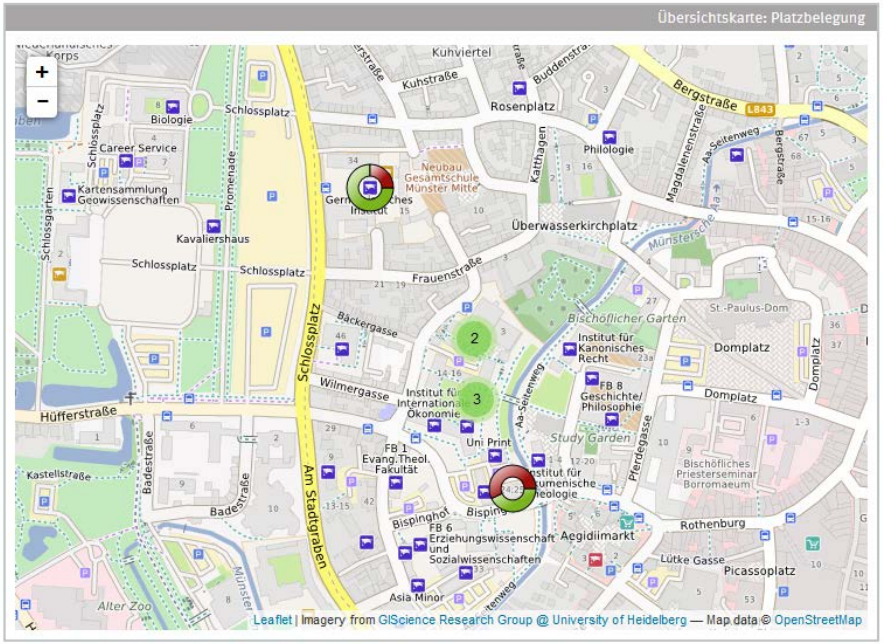


Abb. 2: Graphische Darstellung der verfügbaren Platzticker auf der Website der ULB

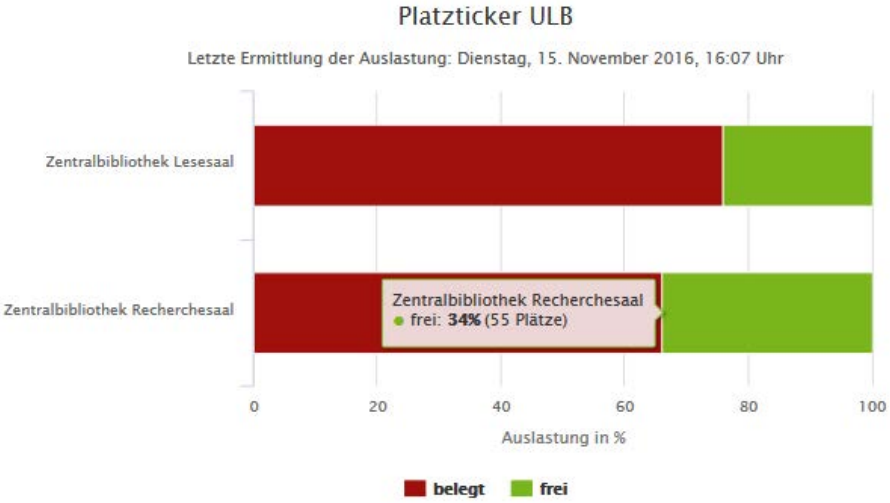


Abb. 3: Platzticker für die Zentralbibliothek der ULB als Balkendiagramm

Die ermittelten Auslastungsquoten werden für die Präsentation auf den Webseiten der ULB und anderer Bibliotheken über eine offene JSON-Schnittstelle zur Verfügung gestellt. Für den Webauftritt der ULB wurde der Platzticker grafisch umgesetzt und umfasst neben einer Übersichtskarte (Abb. 2) auch Statistiken zur Auslastung der einzelnen Standorte (Abb. 3). Für Bibliotheken, die eine Eigenprogrammierung „ihres“ Platztickers auf Basis der JSON-Daten nicht leisten können, stellt die ULB vorkonfigurierte grafische Darstellungen bereit: Ein HTML-Schnipsel mit einem Balkendiagramm der aktuellen Auslastung sowie eine PNG-Graphik mit der Darstellung des zeitlichen Verlaufs der Auslastung am aktuellen Tag sind für jeden Standort abrufbar und können auf einfache Weise in die eigene Website eingebunden werden.

Technische Umsetzung des Platztickers

Der Platzticker der ULB basiert auf einem verlässlichen Proportionalitätsfaktor sowie hochaktuellen WLAN-Login-Zahlen. Die technische Umsetzung dieser Idee ist jedoch komplexer als vielleicht zunächst vermutet:

Für jeden Standort wurde durch manuelle Zählung über einen Zeitraum von mehreren Wochen die tatsächliche Platzbelegung an unterschiedlichen Wochentagen und Uhrzeiten ermittelt. Durch Vergleich mit den gelieferten WLAN-Login-Zahlen konnte damit der Proportionalitätsfaktor für jeden Messzeitpunkt bestimmt werden. Dabei stellte sich heraus, dass der Proportionalitätsfaktor vom Standort und von der Tageszeit abhängt. Insbesondere in der Mittagszeit ist der Proportionalitätsfaktor erhöht, da viele Studierende die Bibliothek für eine Mittagspause verlassen, ohne ihren Arbeitsplatz zu räumen. Deshalb werden in dieser Zeit in Relation zu den belegten Arbeitsplätzen deutlich weniger WLAN-Logins registriert. Für die Kalibrierung des Platztickers bedeutet dies, dass der Proportionalitätsfaktor standortspezifisch als Funktion der Uhrzeit ermittelt und in der Auswertungsroutine hinterlegt werden muss. Die damit abschätzbare absolute Zahl der belegten Arbeitsplätze wird schließlich auf die Gesamtzahl der zur Verfügung stehenden Arbeitsplätze des jeweiligen Standorts bezogen, um die relative Auslastung als Prozentzahl bereitstellen zu können.

Die zweite zentrale Voraussetzung für einen funktionsfähigen Platzticker besteht darin, die Zahl der WLAN-Logins für alle Access-Points der relevanten Räumlichkeiten regelmäßig zu ermitteln und bereitzustellen. Einen solchen Datenexport bietet Cisco Prime, die Steuerungssoftware für die WLAN-Infrastruktur der WWU, allerdings nicht standardmäßig an. Erst ein vom ZIV speziell für diesen Zweck eingerichteter Datenexport ermöglicht es, die Anzahl der Logins für alle benötigten WLAN-Access-Points in Zeitintervallen von fünf Minuten zu protokollieren und dieses Protokoll als strukturierte Textdatei im Webserverpark bereitzustellen. Im nächsten Schritt wurde von der ULB ein Auswertungsskript programmiert, das neu gelieferte Daten im Webserverpark abholt, nach Standorten differenziert auswertet und in eine Datenbank einträgt. Dieses Skript wird bei jedem Web-Aufruf des Platztickers gestartet, sodass stets die aktuellsten Daten zur Anzeige der Auslastung herangezogen werden. Der Eintrag in eine Datenbank erlaubt es zudem, die zeitliche Verteilung der Auslastung für beliebige Zeiträume zu ermitteln und anzuzeigen. Für jeden Standort werden dabei auch die Öffnungs- und Schließzeiten berücksichtigt, um bei geschlossener Bibliothek nicht fälschlich die Anzeige „Anzahl freier Arbeitsplätze = 100 %“ zu generieren.

Groß gegen Klein

Adobe Photoshop und GIMP im Vergleich

von Christopher Burgholz

Adobe Photoshop ist für viele der Inbegriff der Bildbearbeitung. Mittlerweile gibt es jedoch eine Reihe kostenloser Alternativen zu Adobes Software. Eine der bekanntesten Optionen ist das Open-Source-Programm GIMP (GNU Image Manipulation Program), das zu den ältesten und umfangreichsten kostenlosen Grafikprogrammen zählt. Inwiefern es eine Alternative zu Photoshop darstellt und wo die Stärken und Schwächen der beiden Programme liegen, wird in diesem Artikel erläutert.

Auf den ersten Blick fallen die unterschiedlichen Benutzeroberflächen auf. Adobe Photoshop verwendet seit der Version CS eine schwarze bzw. dunkelgraue Oberfläche sowie hellgraue Icons. Visuell macht das Programm einen modernen Eindruck. GIMPs Icons kommen dagegen wesentlich angestaubter daher und nicht zuletzt das GIMP-Maskottchen, das an mehreren Stellen in den Menüs abgebildet wird, wirkt für Neulinge mit Sicherheit eigentümlich. In ihrem Aufbau sind sich die beiden Programme dagegen ähnlich: es gibt ein Anwendungsmenü, eine Werkzeugpalette sowie weitere Bedienfelder. Erfreulich ist, dass Nutzer beider Programme die Bedienfelder neu anordnen und in Gruppen zusammenfassen können. Dies ist bei GIMP auch notwendig, da die Werkzeugleiste standardmäßig dreispaltig und damit viel breiter als nötig ist. Sie beinhaltet darüber hinaus Optionen, die aus der Leiste heraus eigentlich kaum zu verwenden sind und daher vom Nutzer in den Bereich der Bedienfelder verschoben werden sollten.

Die Werkzeugpalette von GIMP ist recht umfangreich. Sie umfasst zentrale Auswahl- und Retusche-Werkzeuge wie beispielsweise den „Zauberstab“ zur automatischen Auswahl zusammenhängender Bildbereiche, den Kopierstempel zum Ausbessern von Fotos und ein ausgeklügeltes „Heilen“-Werkzeug, mit dem Unregelmäßigkeiten in Bildbereichen komfortabel entfernt werden können. Bei Photoshop reicht das Spektrum an Werkzeugen weit über diese Kernelemente hi-

naus und bietet den Nutzern zahlreiche zusätzliche Tools wie zum Beispiel das Schnellauswahl-Werkzeug. Für ein Freeware-Programm verfügt aber auch GIMP über eine sehr gute Ausstattung, die es dem Nutzer ermöglicht unterschiedlichste Bildideen umzusetzen – wenn auch nicht so komfortabel und ausgefeilt wie mit Photoshop.

Erfreulich ist, dass GIMP Ebenen-Masken verwendet, da diese eine wichtige Voraussetzung zum nicht-destruktiven Arbeiten darstellen. Allerdings bietet das Programm kein Äquivalent zu den aus Photoshop bekannten Einstellungsebenen. Diese ermöglichen es dem Nutzer, Farbkorrekturen, Effekte, Kontrastveränderungen und andere Einstellungen auf einer eigenen Ebene auszulagern, die separat von der Bildebene ist. Dadurch kann der Nutzer die Einstellungen jederzeit verändern, ohne dass Bildinformationen dauerhaft überschrieben werden. Prinzipiell lassen sich solche Korrekturen auch in GIMP nicht-destruktiv vollziehen, dies erfordert jedoch das Arbeiten auf duplizierten Bildebenen bzw. innerhalb einer kopierten Bilddatei und ist nicht so effizient wie in Photoshop. Immerhin plant GIMP in der zukünftigen Version 3.2 den Fokus auf nicht-destruktives Arbeiten zu legen – wahrscheinlich werden dann auch Einstellungsebenen eingeführt. Eine Weile wird das aber noch dauern, denn zurzeit ist Version 2.8 aktuell.

GIMPs Stärke gegenüber anderen kostenfreien Programmen liegt im Funktionsumfang. Nutzer können mit verschiedene Maßeinheiten und PPI (Pixel per Inch) arbeiten und Bilder auf diese Weise für Bildschirm und Druck optimieren. Zudem unterstützt GIMP eine Reihe verschiedener Formate beim Dateiexport (u. a. JPEG, TIFF, PDF) und legt so den Grundstein für professionelle Bildschirm- und Druckdateien. Als Marktführer bietet Photoshop jedoch noch wesentlich umfangreichere Exportoptionen: Photoshop-Dokumente können beispielsweise im PDF/X-Standard exportiert werden, der speziell für den Austausch professioneller Druckdaten entwickelt wurde.

Auf ein Gegenstück zu den von Photoshop unterstützen Cloud-Funktionen wie z.B. die Creative Cloud-Bibliotheken werden GIMP-Nutzer wohl auch in näherer Zukunft verzichten müssen. Diese stellen jedoch kein essenzielles Feature dar und sind primär für Nutzer interessant, die Einstellungen zwischen verschiedenen Adobe-Programmen synchronisieren möchten. Darüber hinaus unterstützt Photoshop das Speichern von Dateien in der Creative Cloud sowie damit zusammenhängende Möglichkeiten des kollaborativen Arbeitens. GIMP-Nutzer können hier natürlich kostenlose Alternativen verwenden.

Insgesamt ist GIMP ein gut ausgestattetes freies Bildbearbeitungsprogramm, welches Photoshop in seiner Tiefe zwar nicht das Wasser reichen kann, allerdings einen für ein Freeware-Programm beeindruckenden Funktionsumfang besitzt. Schade ist hingegen, wie angestaubt und eigentümlich die Aufmachung der Benutzeroberfläche daherkommt. Auch die Nutzerführung ist – für ein im Vergleich zu Photoshop eher schlankes Programm – nicht wirklich gelungen. Hier muss GIMP nachbessern, damit das schlechte Interface dem ansonsten soliden Bildbearbeitungsprogramm gerecht wird.

Neue Regelungen zur Privatnutzung von Dienst-Telefon und -Handy

von Dominik Rudolph

Geringfügige Nutzung bei dienstlichen Festnetz-Telefonen erlaubt

Ein kurzer Anruf zu Hause, eine telefonische Terminvereinbarung beim Arzt – wer diese alltäglichen Dinge bisher über ein Telefon der WWU erledigt hat, musste entweder eine zuvor beantragte PIN nutzen oder sich in einen rechtlichen Graubereich begeben. Um für die Beschäftigten rechtliche Sicherheit zu schaffen, haben sich die Personalräte und die Dienststelle der WWU auf eine neue Dienstvereinbarung geeinigt, die das Thema Privattelefonie regelt und viele Verbesserungen für die Beschäftigten enthält. So ist beispielsweise die Beantragung einer persönlichen Vorwahl mit entsprechender Verrechnung nicht mehr erforderlich.

Ähnlich wie bei der Internetnutzung ist nun auch bei Telefonen eine geringfügige Nutzung offiziell gestattet, sofern sie die Dienstgeschäfte nicht beeinträchtigt und sich – außer in dringenden Fällen – auf die Pausenzeiten beschränkt. Um einen Anruf als privat zu klassifizieren, reicht WWU-weit die Vorwahl #99. Dann werden die letzten drei Ziffern der Zielrufnummer anonymisiert. Bei Diensthandys bleibt die private Nutzung dagegen grundsätzlich verboten. Mit TwinPhone steht allerdings ein neues Angebot zur Verfügung, bei dem die Beschäftigten ihr Diensthandy gegen eine geringe Gebühr zeitlich uneingeschränkt auch privat nutzen können.

Aus zwei mach eins: Mit TwinPhone das Diensthandy auch privat nutzen

Wer über ein Diensthandy verfügt, kennt das Problem: Er oder sie muss zwei Geräte mit sich herumtragen, neben dem dienstlichen meist auch noch ein privates Handy. Mit dem neuen TwinPhone-Angebot bietet das ZIV nun eine attraktive Alternative. Gegen Zahlung einer geringen monatlichen Gebühr können Beschäftigte ihr Diensthandy ganz offiziell in der Freizeit für private Zwecke nutzen. Im Preis von 4,52 Euro sind eine Flatrate in alle deutschen Netze (Mobil und Festnetz) sowie ein großzügiges Datenvolumen in Höhe von 1 GB enthalten. Die Gerätekosten trägt wie bisher die WWU. Die private Nutzung ist allerdings auf Deutschland beschränkt. Für das Ausland wird generell die Nutzung einer Prepaid-SIM empfohlen.

TwinPhone ist ein freiwilliges Angebot für Beschäftigte mit einem dienstlichen Handy. Gemäß der neuen Dienstvereinbarung zur Privattelefonie ist die private Nutzung von Diensthandys ohne Abschluss der TwinPhone-Option allerdings nicht gestattet. TwinPhone kann beim ZIV beantragt werden und nach einer Mindestlaufzeit von drei Monaten monatlich gekündigt werden.

Apps mit Uni-Zugangsdaten richtig nutzen

Empfehlungen des IV-Sicherheitsteams

von Thorsten Küfer

Aus Komfort- und Kostengründen bieten Universitäten immer mehr Dienste über das Web an: angefangen bei E-Mails, über Nutzerportale, Vorlesungsunterlagen, Bibliotheks-Recherchen und -Ausleihen bis hin zu Prüfungsanmeldungen und Notenabruf. Viele Dienste liefern sensible Informationen oder erlauben Änderungen an wichtigen Daten und können daher nur nach einer Authentifizierung mit Uni-Kennung und -Passwort genutzt werden. Die Zugangsdaten sind aber nicht nur für die Sicherheit der eigenen Daten sondern auch für den Schutz der Datenverarbeitungsressourcen im IV-System der WWU von besonderer Relevanz und müssen entsprechend geschützt werden. Der richtige Umgang mit Passwörtern spielt hierbei eine entscheidende Rolle und wird auch in der Benutzungsordnung des ZIV thematisiert.

So sind alle Nutzer dazu verpflichtet, ein ausreichend komplexes Nutzerpasswort zu wählen, dieses regelmäßig zu ändern und vor Dritten geheim zu halten. Zum Schutz gegen Phishing und Identitätsmissbrauch empfiehlt das ZIV außerdem, die Uni-Zugangsdaten nur auf Webseiten der WWU einzugeben, die sich per Zertifikat als vertrauenswürdig ausweisen (Aufruf per HTTPS). Immer häufiger werden Passwörter jedoch im Browser oder in Programmen hinterlegt – beispielsweise bei E-Mail-Diensten. Auf PCs und Laptops setzen viele Nutzer Programme wie Outlook oder Thunderbird ein, um auf E-Mails zuzugreifen oder E-Mails zu versenden. Dabei vertrauen sie in der Regel darauf, dass das Programm ihre Passwörter geheim hält. Auch in Browsern ist die Speicherung von Passwörtern zunehmend verbreitet. Für einen höheren Schutz ihrer Zugangsdaten sollten Nutzer hier stets

ein sogenanntes Master-Passwort verwenden (Anleitung für Mozilla Firefox).

Im Bereich von Smartphones und Tablets ist das Angebot an Apps, die den Zugriff auf Informationen erleichtern, längst nicht mehr überschaubar. Oft bestehen diese Programme lediglich aus einem Browser, der mittels gespeicherter Zugangsdaten den Zugriff auf eine Webseite übernimmt. Grundsätzliche Sicherheitsmaßnahmen, wie der Austausch von Daten über HTTPS, werden dabei häufig vernachlässigt. Wenn möglich sollten Nutzer daher den direkten Weg über einen etablierten Browser (Chrome, Firefox) wählen und auf diese Weise sicherstellen, dass keine Daten von Dritten mitgelesen werden. Teilweise ist es für Nutzer auch schwierig, die Vertrauenswürdigkeit einer App oder eines Herstellers einzuschätzen – insbesondere wenn App-Bewertungen im App-Store die einzige Grundlage hierfür darstellen. Ist der Hersteller einer App nicht vertrauenswürdig oder unbekannt, sollten Nutzer dem Programm ihre Daten grundsätzlich nicht überlassen.

Zu berücksichtigen sind darüber hinaus auch Aspekte wie Werbung und das Zwischenspeichern von Daten: So sind die meisten kostenlosen Apps deshalb gratis, weil sie Umsätze über sichtbare oder unsichtbare Werbung generieren – hierfür werden die angezeigten Inhalte analysiert. Durch den teilweise geringen Speicherplatz und die geringe Rechenleistung von Smartphones werden bei der Nutzung von Apps vielfach Daten auf den Servern der Hersteller zwischengespeichert. Anfang 2015 geriet in diesem Kontext Microsoft in die Kritik, da die zugekaufte Outlook App Passwörter und E-Mails auf einem fremden Server zwischenspeichert (Details). Wegen Sicherheitsbedenken wurde die App daraufhin vom EU-Parlament verboten (Details). Insbesondere wenn es um sensible Daten geht, aber auch grundsätzlich, ist bei der Nutzung von Apps also Vorsicht angebracht.

Absicherung von Smartphones

Allgemeine Empfehlungen

- Schützen Sie Ihr Gerät mithilfe eines Passworts bzw. einer PIN.
- Installieren Sie nur Apps aus einem offiziellen App-Store.
- Installieren Sie einen Virenschutz, falls möglich. Er schützt vor böswilligen Apps, die im Hintergrund z. B. kostenpflichtige SMS verschicken oder Telefonate führen.
- Aktivieren Sie die Geräte-Verschlüsselung.
- Vermeiden Sie Jailbreaks/Rooting.
- Nutzen Sie kommerzielle Cloud-Speicher nur für unwichtige Daten und verwenden Sie ggfs. eine Client-seitige Verschlüsselung.

Empfehlungen für Mitarbeiter

- Nutzen Sie das Exchange-System für dienstliche E-Mails, Kontakte und Termine. Das System ermöglicht es, die obigen Empfehlungen automatisch umzusetzen (sofern dies vom Gerät unterstützt wird) und Ihr Gerät bei Verlust aus der Ferne zu löschen.
- Speichern Sie personenbezogene Daten nur auf Servern der Uni Münster.

Neuorganisation der IV-Sicherheit an der WWU

von Thorsten Küfer

An der WWU gibt es bereits seit vielen Jahren Regelungen zur IV-Sicherheit. Diese Regelungen wurden nun auf Basis einer Empfehlung der NRW Landesverwaltung überarbeitet und in einer Informationssicherheitsleitlinie der WWU neu formuliert. Die Leitlinie wurde im Juli 2016 vom Rektorat verabschiedet. Sie ist ein wichtiger Schritt zur Einführung eines Information Security Management Systems (ISMS). Das ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die die Informationssicherheit dauerhaft definieren, steuern, kontrollieren, aufrechterhalten und verbessern sollen. Die WWU bekennt sich damit zu ihrer Verantwortung in der IV-Sicherheit, der Sicherstellung der drei vom BSI definierten Schutzziele: Verfügbarkeit, Vertraulichkeit und Integrität.

Die Zusammensetzung und Aufgaben der bisherigen Organisationseinheiten – IV-Sicherheitsteam und WWU-CERT – werden in der Leitlinie genauer festgelegt. Ein neu besetztes IV-Sicherheitsteams wurde im Oktober 2016 vom IV-Lenkungsausschuss bestätigt und nimmt nun seine Arbeit auf.

IV-Sicherheitsteam

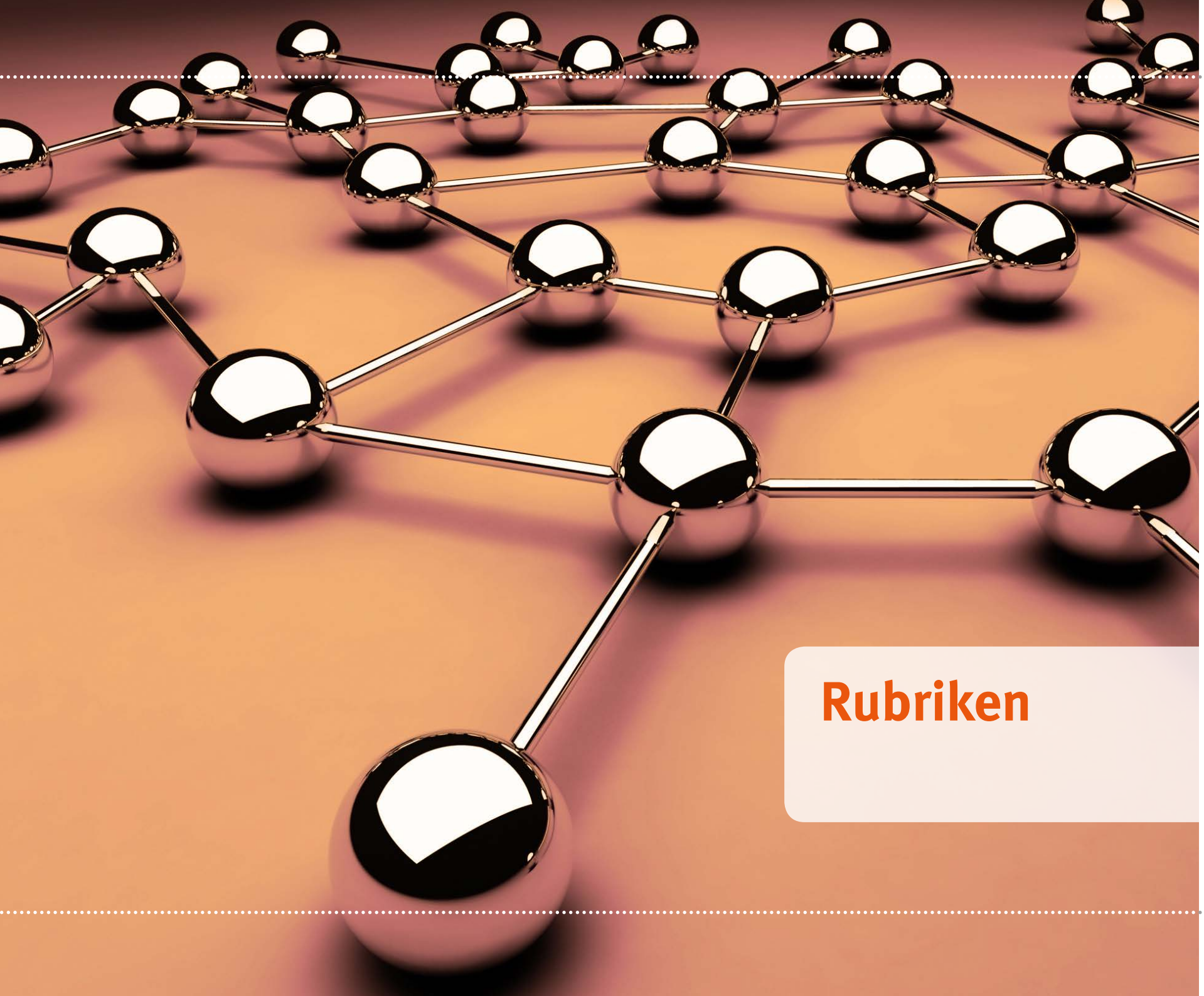
Bereich	Mitglied	Vertreter
Leitung	Thorsten Küfer	Martin Ketteler-Eising
IVV2	Michael Surkau	Pascal Burnus
IVV5	Gerrit Schwerdt	Alexander Preuss
IVV6	Malte Holthaus	Stefan Platz
IVV9	Matthias Rese	Michael Steinkamp
UKM	Ingo Jung	*wird noch benannt*
ZIV Abt. 1	Guido Wessendorf	Markus Speer
	Lutz Elkemann	Dieter Frieler
ZIV Abt. 2	Christian Schild	Matthias Kannengießer
ZIV Abt. 3	Linus Stehr	Nicole Marutz

Neu ist auch die Benennung von IV-Sicherheitsbeauftragten in allen Bereichen der WWU, die als Ansprechpartner für das IV-Sicherheitsteam und die Mitarbeiter des jeweiligen Bereichs fungieren und das IT-Sicherheitsbewusstsein bei den Anwendern fördern sollen. Wenn Sie Fragen oder Hinweise zur IV-Sicherheit haben, wenden Sie sich gerne an Ihren Ansprechpartner vor Ort. Er wird Ihnen nach Möglichkeit direkt helfen oder die Information passend weiterleiten. Das ZIV bietet seit Ende 2016 regelmäßig Schulungen für Mitarbeiter im Rahmen des WWU Weiterbildungsprogrammes an.

Mit dem nun gelegten Grundstein für die Neuorganisation der IV-Sicherheit ist die WWU gut gerüstet, um den Informationssicherheitsprozess weiterzuentwickeln und sich den Cyber-Bedrohungen der Zukunft zu stellen. Weitere Informationen und Praxistipps finden Sie auf den Webseiten zur IV-Sicherheit.

IV-Sicherheitsbeauftragte

Bereich	Mitglied	Vertreter
IVV1	Peter Kollenbrandt	*wird noch benannt*
IVV2	Michael Surkau	Christian Ueding
IVV3	Jens Seipenbusch	*wird noch benannt*
IVV4	Heinz-Hermann Adam	Jürgen Berkemeier
IVV5	Gerrit Schwerdt	Alexander Preuss
IVV6	Malte Holthaus	Stefan Platz
IVV7	Matthias Goden	Thomas Ulbrich
IVV8	Ulrich Janßen	Johann Pelz
IVV9	Matthias Rese	Michael Steinkamp
IVV10/ULB	Christopher Heuermann	Franz Grenzer
UKM	Ingo Jung	Gabriel Rentmeister
ZIV	Thorsten Küfer	Martin Ketteler-Eising



Rubriken

2.350

Das ZIV setzt zur Datensicherung den Tivoli Storage Manager (TSM) ein, der Backup-Daten überwiegend in einem Kassettenarchivsystem speichert. Die auf diese Weise abgelegten Daten haben derzeit ein Volumen von insgesamt 2.350 TB.

Z.I.V.
Zeitschrift zur Informationsverarbeitung an der WWU

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Herausgeber:
Zentrum für Informationsverarbeitung (ZIV)
Röntgenstraße 7–13
48149 Münster

Redaktion: Thorsten Küfer, Stefan Ost, Dominik Rudolph, Markus Speer, Anne Thoring
Gestaltung/Satz: Anne Thoring
Fotografie: Nina Krücken / Julia Koch © ZIV, Christian-P. Worring/Sashkin/32 pixels/skarie/adimas/pixelalex/Dejan Jovanovic/martialred/tom/hd-design © fotolia.com

Telefon: +49 251 83–31600
Fax: +49 251 83–31555

E-Mail: Z.I.V.redaktion@uni-muenster.de
URL: www.uni-muenster.de/ZIV/Z.I.V